

10-11-16
10:45 AM
U.S. DISTRICT COURT
NORTHERN DISTRICT OF OHIO
CLEVELAND

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO
WESTERN DIVISION

LINDSEY WILLIAMS-DIGGINS,
individually and on behalf of all others
similarly situated,

Plaintiff,

v.

MERCY HEALTH, an Ohio non-profit
corporation,

Defendant.

Case No.

3 : 16 CV 1938
JUDGE HELMICK

JURY DEMAND

CLASS ACTION COMPLAINT

Plaintiff Lindsey Williams-Diggins brings this Class Action Complaint against Defendant Mercy Health ("Mercy" or "Defendant") to put an end to Defendant's practice of systematically exposing confidential patient information and storing patient data without adequate security. Plaintiff alleges as follows upon personal knowledge as to himself and his own acts and experiences, and upon information and belief, including investigation conducted by his attorneys, as to all other matters.

NATURE OF ACTION

1. Defendant Mercy is the largest health system in the State of Ohio, with 23 hospitals, dozens of smaller facilities, and over 1,000 physicians located through the state. In 2015 alone, Mercy generated over \$4 *billion* in revenue. As a part of its services, Mercy creates, operates, and maintains websites where employees and patients can access patients' medical data online.

2. Unfortunately, Defendant fails to keep its patients' sensitive medical information secure. Defendant's computer systems suffer from critical vulnerabilities in its internet-accessible web services. As a result, sensitive medical information entrusted to Mercy by its patients has been exposed and is at great risk of further unauthorized disclosure (if it hasn't already been disclosed).

3. Mercy has injured its patients by charging and collecting market-rate medical fees without providing industry standard protections for patient data confidentiality. The longer Mercy is allowed to maintain its vulnerable systems, the more likely its patients will become victims of a data breach. Alternatively, if a breach has already occurred, each day that passes without knowledge and notice of a breach puts patients' sensitive medical information in greater danger of widespread distribution.

4. Accordingly, this putative class action lawsuit seeks (i) to compel Mercy to stop exposing patients' private medical information by implementing industry standard protocols, (ii) to compel Mercy to allow an independent, third-party firm to conduct a security audit, (iii) to inform patients with information stored by Mercy that their information has been exposed, and (iv) attorneys' fees and costs.

PARTIES

5. Plaintiff Lindsey Williams-Diggins is a natural person and citizen of the State of Ohio.

6. Defendant Mercy Health is a non-profit corporation incorporated under the laws of the state of Ohio with a principal place of business at 1701 Mercy Health Place, Cincinnati, Ohio 45237. Defendant conducts business throughout this District, the State of Ohio, and the United States.

JURISDICTION AND VENUE

7. Federal subject-matter jurisdiction exists under 28 U.S.C. § 1332(d)(2) because (a) at least one member of the class is a citizen of a state different from Defendant, (b) the amount in controversy exceeds \$5,000,000, exclusive of interests and costs, and (c) none of the exceptions under that subsection apply to this action.

8. The Court has personal jurisdiction over Defendant because Defendant is registered to conduct business in the State of Ohio, conducts significant business transactions in this District, and because the wrongful conduct occurred in and/or was directed to this District.

9. Venue is proper in this District under 28 U.S.C. § 1391(b) because a substantial part of the events giving rise to Plaintiff's claims occurred in this District, Plaintiff resides in this District, and because Defendant resides in this District.

FACTUAL ALLEGATIONS

I. Introduction to Mercy and its Patient Medical Data Portal.

10. Mercy is the largest health system in the State of Ohio. Mercy employs over 1,000 physicians and 32,000 others in its network of 23 hospitals and dozens of clinics and facilities. Mercy operates in Ohio and Kentucky. Mercy generates more than \$4 billion of revenue per year

and services hundreds of thousands of patients.

11. For each of these patients, Mercy creates and maintains detailed records of health statuses and the treatment provided. While some of these records exist in paper format, Mercy maintains electronic copies of patient medical records and stores those records in its computer systems. Some of these systems are further connected to the internet and act as portals into Mercy's patient data repositories.

12. One such system Mercy has implemented is the Horizon Patient Folder WebStation portal (the "WebStation"), created by non-party McKesson Corporation. McKesson describes the WebStation as a "document management and imaging solution that electronically captures, indexes, completes and stores a legal electronic medical record" and that allows for "[e]asy access to patient information."¹ Mercy's WebStation is publicly available at the addresses: 168-250-52-64.health-partners.org, 168-250-52-65.health-partners.org, and 168-250-52-66.health-partners.org.

13. On these websites, Mercy maintains its patients' private medical information in electronic storage. As such, Mercy is a covered entity under the Healthcare Insurance Portability and Accountability Act ("HIPAA"), which regulates the privacy of patient information.² And, Mercy must comply with HIPAA regulations.

14. Moreover, Mercy regularly receives, maintains, and transmits Protected Health Information, which HIPAA defines as information that is transmitted or maintained in any form or medium, including:

a subset of health information, including demographic information collected from

¹ *OneContent Patient Folder | McKesson*, <http://www.mckesson.com/providers/health-systems/diagnostic-imaging/enterprise-document-management-system/onecontent-patient-folder/> (last visited July 30, 2016).

² 45 C.F.R. § 160.103.

an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.³

15. Mercy recognizes that the patient information it maintains is HIPAA Protected Health information. In its Notice of Privacy Practices, Mercy makes a “Pledge” to patients that it is “committed to protect [their] privacy” and that they are “required by law ... [t]o keep medical information about you private.”⁴

16. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq.* These provisions require, among other things, that the United States Department of Health and Human Services create rules to streamline the standards for handling Protected Health Information, like the data maintained on Mercy’s website.

17. These regulations state that “[a] covered entity or business associate must comply with the applicable standards, implementation specifications, and requirements of this subpart with respect to electronic protected health information of a covered entity.”⁵ Despite making the above promises (and being obligated under law), Mercy does not keep patient’s private medical information confidential.

II. Mercy Has Exposed Patients’ Private Medical Information Without Authorization.

18. Although Mercy represents that it is committed to maintaining patient privacy, it has exposed the private medical information of hundreds of thousands of patients on its websites. Specifically, Mercy’s network connected patient medical information portals (e.g., WebStation)

³ *Id.*

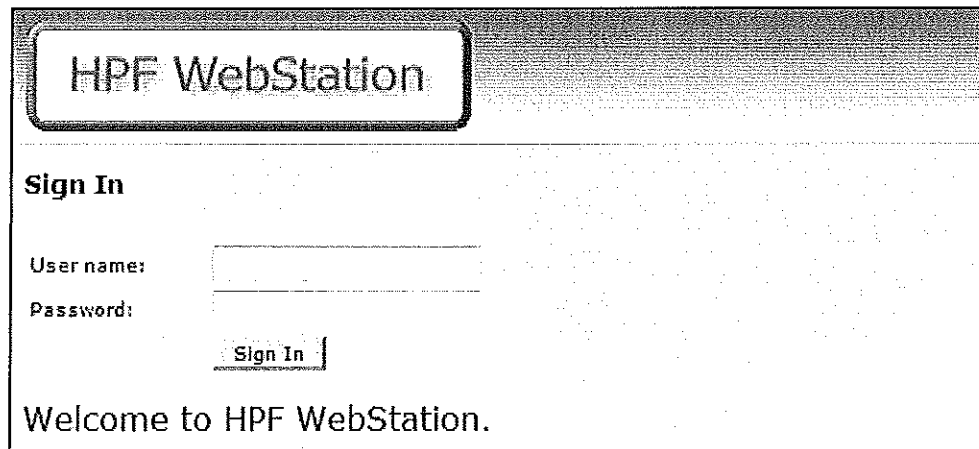
⁴ A true and accurate copy of Defendant’s Notice of Privacy Practices is attached hereto as Exhibit A.

⁵ 45 C.F.R. § 164.302.

lack basic and fundamental security safeguards and are vulnerable to hacks and further disclosure of confidential medical information.

A. Mercy's WebStation Stores Patients' Sensitive Medical Information.

19. Through its WebStation, Mercy allows its employees and agents to access patients' medical information. Defendant Mercy owns and operates the websites 168-250-52-64.health-partners.org, 168-250-52-65.health-partners.org, and 168-250-52-66.health-partners.org where it provides access to its WebStation. Defendant's employees seeking access to patient medical records can use an internet browser (i.e., Google Chrome or Mozilla Firefox) to navigate to a WebStation addresses (e.g., 168-250-52-64.health-partners.org). Once at that website, Defendant's servers load a login prompt where employees are required to enter their usernames and passwords to proceed. *See Figure 1.*



(Figure 1.)

20. Upon entering a valid username and password, Defendant's systems will present the authorized employee or agent with a screen similar to the one shown in Figure 2. There, the user is able to conduct searches of patients' sensitive medical information, amongst other things.

(Figure 2.)⁶

21. For instance, the health information contained in Defendant's WebStation service seemingly includes the patients' name, admission date, status, date of birth, age, and additional demographic information. *See* Figure 3.

✓	P	B	V	A	Patient Name	AT	Nursing Station	Room/Bed	Complaint	Admit Date	Discharge Date	Status	DOB	Age	S	Visit ID	HRH	
<input type="checkbox"/>					BEAUTY, SLEEPING	G	UNKNOWN LOCATION	UNASSIGNED	sleep lab // acute sleep study apnea	04/10/2013 21:00		Pre-Reg	12/31/1974	38Y	F	3000000410	100179885	OUTP
<input type="checkbox"/>					BIPACONE, SEAR	G	2504TH	2206-D	depression	04/02/2013 12:00		Admit	03/01/1950	63Y	M	3000000356	100179798	INPA
<input type="checkbox"/>					BIPACTWO, HAZEL	G	3AEST	303-B	CHEST PAIN	04/02/2013 12:30		Admit	03/12/1965	47Y	M	7000000341	100175809	INPA

(Figure 3, showing sample WebStation data.)⁷

22. The WebStation also stores detailed medical records, such as a patient's diagnosis, treatment, and even specific laboratory results:

⁶ HealthAlliance of Hudson Valley, *PHYSICIAN Instructions: Paragon's WebStation for Physicians*, 1, available at <http://home.hahv.org/Access/MedicalStaff/Physician/Doctor%20instructions%20Webstation%20for%20physicians.pdf>.

⁷ *Id.* at 2.

(7) Results (Save/Restore)				
Laboratory		Radcliff	Cardiology	Other
<input type="button" value="back"/> <input type="button" value="=<"/> <input type="button" value="=>"/> <input type="button" value="trend"/> <input type="button" value="reorder"/>				
A. Visit ID: 2000000149 Name: HPF, MDSGFIVE Collected: 03/15/2013 15:01 Priority: Routine		Order # 5 Result Status: Final Report Released: 03/15/2013 17:05 Body Site:		Description: DIFFERENTIAL WBC COUNT Ordered By: FRISS, LEANNE Event: 03/14/2013 10:35 Specimen Source:
<input checked="" type="checkbox"/>	Result Name	Results	Reference Range	UOM
<input type="checkbox"/>	NEUTROPHIL PERCENT	50.0	40.0-74.0	%
<input type="checkbox"/>	LYMPHOCYTE PERCENT	40.0	19.0-46.0	%
<input type="checkbox"/>	MONOCYTE PERCENT	5.0	3.4-9.0	%
<input type="checkbox"/>	EOSINOPHIL PERCENT	3.1	0.0-7.0	%
<input type="checkbox"/>	BASOPHIL PERCENT	1.9 H	0.0-1.5	%

(Figure 4, showing sample laboratory results for fictional “Leanne Friss.”)⁸

23. Defendant’s system, though, does not limit access to individuals with valid usernames and passwords. Instead, hackers can breach its system with impunity because Defendant has improperly configured the service and left it running out-of-date software. A review of the publically available specifications of Defendant’s WebStation service shows that it is more than a decade old and has not been updated with critical security patches.

B. *Mercy’s WebStation leaves patients’ private medical information exposed.*

24. Defendant’s WebStation patient information portal is built on a “JBoss Application Server” which implements Java (a virtual computing language) for applications. By using Java, service providers are able to let users run applications on myriad devices without having to rewrite the application for each type device (*e.g.*, a Java application can run on a Mac and a PC without modification).

25. Mercy’s implementation of JBoss is woefully out-of-date and suffers from a critical vulnerability (the “JBoss Vulnerability”). Defendant’s JBoss system is listed as running version 5.0. A review of industry literature reveals that that version of JBoss was introduced in

⁸ *Id.* at 5.

2008 and is nearing “End of Life,” or, no longer supported or recommended for use. For comparison, the latest version of JBoss (now called WildFly) is version 10.

26. In September 2013, the National Institute of Standards and Technology, sponsored by the Department of Homeland Security, updated its National Vulnerability Database to include a vulnerability specific to this version of JBoss. NIST reported that the vulnerability was “network exploitable,” had a “low” level of access complexity, and that it “[a]llows unauthorized disclosure of information; [a]llows unauthorized modification; [and a]llows disruption of service.”⁹ That is, JBoss version 5.0 allows hackers to access previously protected information with little to no effort.¹⁰

27. The risk of this vulnerability is not just theoretical. Computer security experts have recently observed an ongoing and “widespread campaign” attacking JBoss computer systems of the exact type used by Defendant.¹¹ In these attacks, “[a]dversaries are exploiting known vulnerabilities in unpatched JBoss servers [just like Defendant’s out-of-date servers] before installing [malicious software], identifying further network connected systems, and installing SamSam ransomware to encrypt files on these devices.” That is, hackers are targeting entities that have not updated their JBoss servers and then holding sensitive data hostage until a ransom is paid.

28. On April 4, 2016, a user commented about this attack with the following:

⁹ NVD – Detail, <https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-4810> (last visited Aug. 1, 2016); *Does CVE-2013-4810 affect Red Hat JBoss products? - Red Hat Customer Portal*, <https://access.redhat.com/articles/545183> (last visited July 30, 2016).

¹⁰ Specifically, Mercy’s JBoss implementation has been misconfigured in a way that users can access the “JMXInvokerServlet” and “EJBInvokerServlet” JBoss “servlets” (i.e., server interfaces) without authorization.

¹¹ *Cisco Talos Blog: SamSam: The Doctor Will See You, After He Pays The Ransom*, <http://blog.talosintel.com/2016/03/samsam-ransomware.html?m=1> (last visited Aug. 1, 2016).

We were hit by this ransomware and I wasn't sure if it was jboss related or a compromised user account. Good to at least know it was jboss related. We had port 443 open to the world on an aging server :¹²

That user, just like Mercy, ran an outdated server that was exposed to the internet ("port 443 open to the world") and was attacked.

29. Vulnerabilities like the one Mercy has on its WebStation often serve as the entry point to other sensitive and potentially vulnerable systems. Mercy undoubtedly has a host of network connected medical devices in its hospital systems that may be vulnerable to hackers, including MRI machines¹³, drug infusion machines¹⁴, and robotic surgical equipment¹⁵. Each of those systems might suffer from their own vulnerabilities (or may not be protected by any mechanism at all) and if a hacker gains access to them, he or should could tamper with at-risk patients and the delivery of vital medical care.

30. For instance, a service related to the WebStation service has a vulnerability that *cannot* be remedied: "The McKesson Horizon Clinical Infrastructure (HCI) software uses common, hardcoded passwords for the Oracle database. A remote user with knowledge of the

¹² *Id.*

¹³ *Medical devices could be lethal in hands of hackers | TheHill*, <http://thehill.com/policy/cybersecurity/271003-medical-devices-could-be-lethal-in-hands-of-hackers> (last visited July 30, 2016) (stating that "Hackers could disable a certain commonly used piece of equipment, like an MRI machine, effectively withholding needed care.")

¹⁴ *Medical Devices That Are Vulnerable to Life-Threatening Hacks | WIRED*, <https://www.wired.com/2015/11/medical-devices-that-are-vulnerable-to-life-threatening-hacks/#slide-1> (last visited July 30, 2016) (noting that researchers "found vulnerabilities in the pump that would allow a hacker to surreptitiously and remotely change the amount of drugs administered to patients to deliver a deadly dosage.")

¹⁵ *Telesurgery Vulnerable to Remote Hacks, Hijacks*, <https://blog.kaspersky.com/hacking-robotic-surgeons/8570/> (last visited July 30, 2016) (stating that "A group of academic security researchers remotely hacked and took control of a robot designed to perform telesurgery.")

passwords can connect to the target database.”¹⁶ That is, every instance of McKesson’s HCI software (e.g., installed in different hospitals across the country) uses the *same* password and entities cannot change that password. Should a hacker gain access through Mercy’s JBoss Vulnerability, there are few (if any) additional security measures to protect against further unauthorized access and disclosure of highly sensitive patient medical information.

31. Making matters worse, Mercy has likely been notified by McKesson that the WebStation is vulnerable and should not be used to store patients’ private medical information. Lovelace Hospital system of New Mexico also utilizes the WebStation system from McKesson and issued the following notice on its webpage:

We are beginning the upgrade of the medical records system, Horizon Patient Folder, to McKesson One Content on July 24th, 2016. The go-live of this product has brought to light a potential security risk that needs to be mitigated in order to protect our patient data and remain in compliance with HIPAA guidelines. You will be able to access the

(Figure 5.)¹⁷

32. There, just as here, Lovelace Hospital System runs the Horizon Patient Folder built by McKesson. And, Lovelace’s HPF—just like Mercy’s still does—suffered from a “potential security risk” that if left unfixed would have resulted in Lovelace not being “in compliance with HIPAA guidelines.”

33. It is just a matter of time until a hacker discovers Mercy’s vulnerable system and further exposes patients’ private medical information. As such, the consequences of Defendant’s

¹⁶ *McKesson Horizon Products Use Hardcoded Database Passwords That May Allow Remote Users to Access the System – SecurityTracker*, <http://securitytracker.com/id/1023050> (last visited July 30, 2016).

¹⁷ A true and accurate screenshot of the webpage *HorizonWP Physician Portal*, <https://myportal.lovelace.com/portal/site/nonss/> as it appeared on July 18, 2016 is attached hereto as Exhibit B.

failure to adequately secure patients' private medical information cannot be overstated: with only minimal effort, a hacker can gain access to an immense amount of private medical data. Worse, it may be possible for the hacker to edit or delete sensitive patient information, putting patients' health and safety at high risk.

C. Mercy ignores industry standards, leaving patients' private medical information exposed.

34. If Mercy were to follow industry standards, patients' private medical information would not be exposed. Industry standard practices (and common sense) dictate that only verified Mercy employees (e.g., physicians and medical personnel) should be granted access to patients' private medical information and that all others should be prohibited from accessing that information. Myriad methods exist to ensure that does not happen on even the most basic of websites and services. For websites that maintain sensitive information, such as medical records, there exist governmental organizations, industry groups, and others that recognize the heightened demand for security and, as such, outline protocols to ensure data integrity.

35. Broadly speaking, by exposing patients' private health information, Mercy has failed to implement industry standard user verification techniques and data security as required by federal law, among other things. More specifically, Mercy:

- a. Fails to maintain an adequate data security system to prevent data breaches;
- b. Fails to mitigate the risks of a data breach and unauthorized access to protected health information;
- c. Fails to encrypt or otherwise protect Plaintiff's and the Class's protected health information;
- d. Fails to ensure the confidentiality and integrity of electronic protected health information it created, received, maintained, and transmitted in violation of 45 C.F.R. § 164.306(a)(1);

- e. Fails to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);
- f. Fails to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);
- g. Fails to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R. § 164.306(a)(2);
- h. Fails to protect against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);
- i. Fails to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(4);
- j. Fails to effectively train all members of its workforce on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of protected health information in violation of 45 C.F.R. § 164.530(b); and
- k. Fails to design, implement, and enforce policies and procedures establishing administrative safeguards to reasonably safeguard protected health information, in compliance with 45 C.F.R. § 164.530(c).

36. Mercy also fails to comply with industry standards. Over a decade ago, in March 2005, the National Institute of Standards and Technology (“NIST”) published a report detailing standards for healthcare providers seeking to comply with HIPAA’s Security Rule. In the report, NIST recommended specific techniques to safeguard electronically stored sensitive information. In one example, NIST specifically recommended that companies use “authentication mechanisms [] to verify the identity of those accessing systems protected from inappropriate manipulation.”¹⁸

¹⁸ Matthew School et al., National Institute of Standards and Technology, U.S. Dep’t of Commerce, *NIST Special Publication 800-66 Revision 1: An Introductory Resources Guide for*

37. In addition, the United States Department of Health and Human Services (“HHS”) has issued many documents to assist covered entities better secure patient data. In a white paper on “Security Standards: Technical Safeguards,” the HHS explains that:

In general, authentication ensures that a person is in fact who he or she claims to be before being allowed access to [electronic protected health information (“EPHI”)]. This is accomplished by providing proof of identity. There are a few basic ways to provide proof of identity for authentication. A covered entity may:

- Require something known only to that individual, such as a password or PIN.
- Require something that individuals possess, such as a smart card, a token, or a key.
- Require something unique to the individual such as a biometric. Examples of biometrics include fingerprints, voice patterns, facial patterns or iris patterns.

Most covered entities use one of the first two methods of authentication. Many small provider offices rely on a password or PIN to authenticate the user. If the authentication credentials entered into an information system match those stored in that system, the user is authenticated. Once properly authenticated, the user is granted the authorized access privileges to perform functions and access EPHI.¹⁹

38. Mercy ignores many other long-standing industry protocols, including the standard practice of regular auditing and monitoring of systems that protect sensitive information. In 1996, NIST issued the “Principles and Practices for Security IT Systems,” and while many specific technologies have changed since that document’s release, the underlying guidelines have stayed the same.²⁰ For instance, once a system has been deployed, organizations are to conduct “[a] system audit [which] is a one-time or periodic event to evaluate security” and

Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (Oct. 2008), at 23, available at <http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf>.

¹⁹ Department of Health and Human Services, *HIPAA*, <http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf> (last visited July 30, 2016).

²⁰ U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology, *Generally Accepted Principles and Practices for Security Information Technology Systems*, 24 (available at <http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf>).

to “monitor[] ... ongoing activity [to] examine[] either the system or the users.”²¹ One audit specifically mentioned (and used more commonly in the industry today) is “Penetration Testing,” which is described as follows:

Penetration testing can use many methods to attempt a system break-in. In addition to using active automated tools as described above, penetration testing can be done “manually.” For many systems, lax procedures or a lack of internal controls on applications are common vulnerabilities that penetration testing can target. Penetration testing is a very powerful technique; it should preferably be conducted with the knowledge and consent of system management.²²

39. If Mercy conducted even a basic penetration test to look for cyber security weaknesses, it would have uncovered the JBoss Vulnerability. The nature of the JBoss Vulnerability (i.e., that it is caused by a misconfigured file) suggests that Mercy’s system has been vulnerable since it first implemented WebStation, many years ago. Had Mercy conducted any penetration testing over that time, it would have been alerted that its systems are vulnerable.

40. And, if implements even one of the above security procedures, patient data will no longer be exposed. But despite the foregoing, Mercy does not employ any of the above safeguards. Nevertheless, Mercy has reason to know that patient data should be kept confidential, as HIPAA and industry-standard protections (which Mercy ignores) exist *specifically* to prevent unauthorized access to patients’ private medical information and maintain that data’s integrity.

41. Mercy’s actions are alarming. Mercy patients both expect and pay for (as a part of their medical payments) the confidentiality of their private medical information as part of receiving and paying for medical treatment, but Mercy has exposed that information. Moreover, Mercy has profited by not allocating necessary resources to keep information confidential (e.g., by implementing industry standard information security).

²¹ *Id.*

²² *Id.* at 25.

III. Patient Medical Information is a Primary Target for Hackers.

42. Patients are not only faced with the present injury of Mercy exposing their private medical information, but the longer Mercy leaves their information in the open, the more likely the patients are to become victims of further harm, including identity theft and physical harm from altered medical records. As stated, Mercy is a massive data breach waiting to happen.

43. This risk is especially great for Mercy, considering the sensitive type of information with which it has been entrusted. While companies of all sizes are increasingly at risk of having sensitive information stolen, the risk is exacerbated in the medical industry as patients' private medical records become digitized. Identity thieves have specifically targeted private medical information because that data is more valuable than other types, such as even credit card numbers. As a result, medical organizations and companies that provide services to those organizations have been specifically warned to strengthen security measures.

44. In a June 2007 report on data theft, the United States Government Accountability Office noted that identity thieves use stolen information to open financial accounts, receive government benefits, and incur charges and open credit in a person's name.²³ As the report states, this type of identity theft is the most harmful because it may take some time for the victim to become aware of the theft, which can adversely impact the victim's credit rating. Victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name."²⁴

45. Worse, a person whose personal information has been compromised may not see any signs of identity theft for years:

²³ See United States Government Accountability Office, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), available at www.gao.gov/new.items/d07737.pdf.

²⁴ *Id.*

“[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.”²⁵

46. Stolen medical information is a valuable commodity to identity thieves who often trade the information on cyber black-markets. Indeed, entire online “underground exchanges” have been created “where hackers sell [stolen] information,” such as “names, birth dates, policy numbers, diagnosis codes and billing information.”²⁶ On these exchanges, “medical information is worth 10 times more than [] credit card number[s].”²⁷ One report noted that “[h]ealth insurance credentials are especially valuable in today’s economy because health care costs are causing people to seek free medical care with these credentials.”²⁸

47. Examples of medical data breaches are legion. The U.S. Department of Health and Human Services Office for Civil Rights maintains an up-to-date list of every reported “breach[] of unsecured protected health information affecting 500 or more individuals.”²⁹ At last count, there were over 1,600 reported incidents since October 2009—more than one breach every other day.³⁰ In one recent case, a “niche pharmaceutical company” suffered a breach of “50,000 records” and was being held ransom by a “hacker who [was looking] to sell the data to

²⁵

Id.

²⁶

Your medical record is worth more to hackers than your credit card | Reuters, www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924 (last visited July 25, 2016).

²⁷

Id.

²⁸

Why hackers want your health care data most of all | InfoWorld, www.infoworld.com/article/2983634/security/why-hackers-want-your-health-care-data-breaches-most-of-all.html (last visited July 25, 2016).

²⁹

U.S. Department of Health & Human Services - Office for Civil Rights, ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited July 25, 2016).

³⁰

Id.

the highest bidder or back to the company, whichever comes first.”³¹

48. In another example from September of 2015, Systema Software, a company that works with physicians and clinics to provide access to patients’ medical information over the internet (not unlike Mercy), improperly secured the private medical information of approximately 1.5 *million* patients.³² There, Systema Software apparently failed to implement industry-standard authentication protocols, allowing a “self-described ‘technology enthusiast’” to breach its systems to access and download patients’ “name, Social Security Number, phone number, address,” “financial transaction data,” and “insurance claim forms with some medical/health information.” Had Systema Software implemented basic security features, the breach would have been thwarted. As it stands, the company joins the growing list of companies that have been breached.

49. In fact, the American Bar Association published a book warning companies that store patient data that “[m]assive data breaches are occurring with alarming frequency. An analysis of data breaches by industry should provide a wake-up call for the health care industry.”³³ The ABA went on, saying that “[f]ailed security has resulted in massive data breaches that led to the loss or compromise of millions of personally identifiable health care records. ... In almost all cases, data breaches that occurred could have been prevented by proper planning and the correct security design and implementation of appropriate security

³¹ *Akorn Inc. has customer database stolen, records offered to highest bidder* | CSO Online, www.csoonline.com/article/2938032/data-breach/akorn-inc-has-customer-database-stolen-records-offered-to-highest-bidder.html (last visited July 30, 2016).

³² *Oops! Error by Systema Software exposes millions of records with insurance claims data and internal notes (Update2)*, <http://www.databreaches.net/oops-error-by-systema-software-exposes-millions-of-records-with-insurance-claims-data-and-internal-notes/> (last visited July 30, 2016).

³³ *Health Care Data Breaches and Information Security*, www.americanbar.org/content/dam/aba/publications/books/healthcare_data_breaches.authcheckdam.pdf (last visited July 30, 2016).

safeguards.”³⁴

50. As such, companies entrusted with sensitive patient medical information must be vigilant against threats and employ (at a bare-minimum) industry-standard cyber protection. Any cost borne by the company to implement those practices is dwarfed by the cost faced by consumers who are victim to a medical data breach. The “average total cost” of medical identity theft is “about \$20,000” per incident, according to a report by Experian, and the majority of victims of medical identity theft are forced to pay out-of-pocket costs for health care they did not receive (*i.e.*, fraudulent medical billing and services) just to restore medical or insurance coverage.³⁵ Indeed, almost half of medical identity theft victims lose their health care coverage as a result of such incidents, nearly one-third will see their insurance premiums rise, and forty percent are likely to never to get closure of their identity theft.³⁶ Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole.

51. Importantly, the disclosure and theft of medical data has effects far beyond money costs, including dangerous physical consequences and reputational harm. In 2014, CBS News reported that “[m]edical identity theft can threaten health as well as bank account[s].”³⁷ The report went on to state that “15 percent of the medical identity theft victims surveyed reported that the theft had created misinformation in their medical records that led to a misdiagnosis, and 14 percent said they experienced a delay in care.”³⁸ Because of this, “[t]he impact of medical

³⁴

Id.

³⁵

See Elinor Mills, *Study: Medical identity theft is costly for victims*, news.cnet.com/8301-27080_3-10460902-245.html (last visited July 30, 2016).

³⁶

Id.

³⁷

Experts say medical identity theft is “low-hanging fruit” for thieves; cite limited police attention and lack of record-keeping - CBS News, <http://www.cbsnews.com/news/medical-identity-theft-can-threaten-health-as-well-as-bank-account/> (last visited July 30, 2016).

³⁸

Id.

identity theft can be even more dire than financial identity theft.”³⁹

52. And in a February 2015 study, the Ponemon Institute—a group “dedicated to independent research and education that advances responsible information and privacy management practices within business and government”—reported that “medical identity theft affected [victims’] reputation mainly because of embarrassment due to disclosure of sensitive personal health conditions.”⁴⁰ Ponemon went on to report that the disclosure of that potentially embarrassing personal health information has led victims to “miss out on career opportunities” and lose their jobs.⁴¹

53. And if these warnings against and dire consequences of disclosing sensitive health-related data were not enough, Mercy is specifically on notice that hackers and identity thieves target its patients’ private medical information stored on its servers. On March 28, 2014, Mercy disclosed that employees of one of its hospitals “responded to ‘phishing’ emails that appeared legitimate” and then “disclosed the demographic and clinical protected health information (PHI) of approximately 2,992 individuals.”⁴² From this event, it is also evident that Mercy lacked (and likely still lacks) safeguards for patient data: Mercy’s employees were not trained to detect hack attempts, Mercy’s systems were not sufficient to detect simple email phishing hacks, and Mercy’s operational control did not prevent the unauthorized disclosure of

³⁹ *Id.*

⁴⁰ Ponemon Institute, *Fifth Annual Study on Medical Identity Theft*, (Feb. 2015) available at http://medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf

⁴¹ *Id.*

⁴² U.S. Department of Health & Human Services - Office for Civil Rights, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited July 30, 2016) (showing results of “CE / BA Name Search” for “Jewish Hospital”). In 2015, Mercy was also involved in the largest data breach in Ohio where 113,000 were “inadvertently disposed of ... in a public recycling bin.” Springfield hospital data breach largest in Ohio | News, <http://www.daytondailynews.com/news/news/local/springfield-hospital-records-breach-largest-in-ohi/nqbgY/> (last visited July 30, 2016).

3,000 patients' confidential medical information.

54. Given Defendant's track record and the recognized targeting of patient data by identity thieves, it is likely that the confidential patient data entrusted to—and posted online with *no* data security protections by—Defendant may have already been compromised and misused. Mercy's websites have been operating for months (at least) with the vulnerabilities described here. And because of poor security management and administration, there is a strong chance that Mercy is ignorant of prior or continuing unauthorized access/use stemming from the website vulnerabilities.

55. As such, the only way to protect Plaintiff's and other similarly situated patients' confidential patient data is through an injunction compelling Defendant to immediately disconnect its servers from external networks (*e.g.*, the internet) until it can at least implement basic industry standard protections to keep that information confidential, and to allow an independent third-party firm to conduct a security audit its systems to ensure the integrity of patients' private medical information and determine the extent of any data breach that may have already occurred.

PLAINTIFF WILLIAMS-DIGGINS'S EXPERIENCE

56. Plaintiff Williams-Diggins has been a patient at Mercy affiliated facilities for more than a decade, and has regularly visited a Mercy affiliated clinic in Maumee, Ohio. During that time, Plaintiff received care and Mercy created electronic records of Plaintiff's visits. Plaintiff routinely paid (directly through deductibles and/or copays and indirectly through his insurance premiums) for the medical care he received.

57. Plaintiff paid for the medical care he received because he had the reasonable expectation that Mercy was keeping his medical information confidential. Moreover, Plaintiff

understood and expected that companies entrusted with private medical information are required by law (*e.g.*, HIPAA) to use industry standard security protections to safeguard the data and keep it confidential. Plaintiff values the privacy of his private medical information and avoids doing business with companies with lax data security protocols.

58. Presently, Plaintiff's private medical information is being maintained on Mercy's servers and is been exposed without his authorization.

CLASS ALLEGATIONS

59. **Class Definitions:** Plaintiff brings this class action pursuant to Fed. R. Civ. P. 23(b)(1), (b)(2), and (b)(3) on behalf of himself and a Class and Subclass of similarly situated individuals, defined as follows:

Class: All persons in the United States who have received medical care at a Mercy facility and who have their medical information stored electronically by Defendant.

Ohio Subclass: All individuals in the Class who are domiciled in the State of Ohio.

The following persons are excluded from the Class and Ohio Subclass ("the Class"): (1) any Judge or Magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which the Defendant or its parents have a controlling interest and their current or former employees, officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

60. **Numerosity:** On information and belief, tens of thousands of consumers fall into the Class definition. Members of the Class can be identified through Defendant's records.

61. **Commonality and Predominance:** Common questions of law and fact exist as to all members of the Class and, pursuant to Fed. R. Civ. P. 23(b)(3), predominate over any questions affecting only individual members. Those questions with respect to the Class include, but are not limited to:

- (a) Whether Mercy has exposed its patients' private medical information;
- (b) Whether Mercy fails to adequately secure patients' private medical information;
- (c) Whether Mercy has breached its contracts with Plaintiff and members of the Class;
- (d) Whether Mercy has violated the Ohio Consumer Sales Protection Act;
- (e) Whether Mercy has been unjustly enriched;
- (f) Whether Mercy has breached the confidence of Plaintiff and the Ohio Subclass; and
- (g) Whether Plaintiff and the Class are entitled to a permanent injunction to protect their private medical information.

62. **Typicality:** Plaintiff's claims are typical of the claims of other members of the Class, in that Plaintiff and the members of the Class continuously sustain injury arising out of Defendant's wrongful conduct.

63. **Adequate Representation:** Plaintiff will fairly and adequately represent and protect the interests of the Class and has retained counsel competent and experienced in complex litigation and class actions. Plaintiff's claims are representative of the claims of the other members of the Class. That is, Plaintiff and the Class members each have their private medical information insecurely stored on Defendant's servers and require an injunction to safeguard their

data and have paid for Mercy's services with a portion of each payment to be uses for the administrative costs of data management and security. Plaintiff also has no interests antagonistic to those of the Class, and Defendant has no defenses unique to Plaintiff. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of the members of the Class, and have the financial resources to do so. Neither Plaintiff nor his counsel have any interest adverse to the Class.

64. **Policies Generally Applicable to the Class:** This class action is appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the members of the Class and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies that Plaintiff challenges apply and affect members of the Class uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff. The factual and legal bases of Defendant's liability to Plaintiff and to the other members of the Class are the same.

65. **Separate Suits Would Create Risk of Varying Conduct Requirements:** The prosecution of separate actions by members of the Class against Mercy would create a risk of inconsistent or varying adjudications with respect to individual members of the Class that would establish incompatible standards of conduct. Certification is therefore proper under Fed. R. Civ. P. 23(b)(1).

66. **Appropriateness of Injunctive Relief:** Pursuant to Fed. R. Civ. P. 23(b)(2), Defendant has acted on grounds generally applicable to the Class, thereby making final injunctive relief appropriate with respect to the Class as a whole. Prosecution of separate actions

by individual members of the Class would create the risk of inconsistent or varying adjudications with respect to individual members of the Class that would establish incompatible standards of conduct for Defendant.

67. **Superiority:** This case is also appropriate for certification, pursuant to Fed. R. Civ. P. 23(b)(3), because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy. The harm suffered by the individual members of the Class is likely to have been relatively small compared to the burden and expense of individual prosecution of litigation to redress Defendant's actions. Absent a class action, it would be difficult if not impossible for the individual members of the Class to obtain effective relief from Defendant. Even if members of the Class themselves could sustain such individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties and the Court and require duplicative consideration of the legal and factual issues presented. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single Court. Economies of time, effort, and expense will be fostered and uniformity of decisions will be ensured.

68. Plaintiff reserves the right to revise the foregoing "Class Allegations" and "Class Definition" based on facts learned through additional investigation and in discovery.

COUNT I
Breach of Contract
(On behalf of Plaintiff and the Class)

69. Plaintiff incorporates by reference the foregoing allegations as if fully set forth herein.

70. Plaintiff and Class members entered into contracts with Defendant to receive medical care. The terms of the contracts are found, in part, in Defendant's Notice of Privacy Practices, as described in Section I. *See* Exhibit A.

71. As detailed in this Complaint, Defendant has breached the above contracts by exposing Plaintiff's and the Class's private medical information. In addition, Mercy continuously breaches the above contracts by failing to safeguard Plaintiff's and the Class's private medical information.

72. At all times relevant to this action, Defendant acted willfully and with intent to breach contracts entered into with Plaintiff and the Class. Specifically, Mercy (and its website developers and network security employees) programmed its websites and designed and configured them with inadequate safeguards.

73. Plaintiff and the Class have fully performed their contractual obligations.

74. As a direct and proximate result of Defendant's breach and continuing breach of contract, Plaintiff and the Class have been injured. Specifically, Plaintiff and the Class have been injured because Mercy has exposed their private medical information on its websites; they have suffered a diminished value of the Mercy services they received; and they are threatened with irreparable loss of the integrity of their private medical information and further injury and damages from the theft of that information.

75. Defendant's breach will continue unless enjoined by this Court. Plaintiff and members of the Class are likely to succeed on the merits, are without adequate remedies at law, are threatened with irreparable loss, injury, and damages unless the Court grants the equitable relief requested, and the equitable relief requested is also in the public interest.

76. Plaintiff and members of the Class will suffer substantially more from the denial

of an order enjoining Defendant from further unfair or deceptive conduct than the Defendant would suffer from its issuance.

77. As such, Plaintiff and the Class request that the Court enjoin Defendant from operating its network connected patient medical information portals (e.g., WebStation) until it implements industry standard security protocols to protect their private medical information and from connecting its servers to external networks (e.g., the internet). In addition, Plaintiff and the Class seek an order compelling Defendant to inform patients who have their private medical information accessible on Defendant's websites that they face a threat of further unauthorized disclosure due to Mercy's substandard security measures.

COUNT II
Unjust Enrichment
(In the alternative to Count I)
(On behalf of Plaintiff and the Class)

78. Plaintiff incorporates by reference the foregoing allegations as if fully set forth herein.

79. Plaintiff hereby pleads Count II in the alternative to Count I.

80. Plaintiff and members of the Class conferred a measurable monetary benefit on Defendant. Defendant received and retained money belonging to Plaintiff and the Class in the form of a portion of the medical fees paid to Mercy.

81. Defendant appreciates or has knowledge of such benefit.

82. A portion of the medical fees that Plaintiff and the Class paid to Defendant was to be used by Mercy, in part, to pay for the administrative costs of data management and security (*i.e.*, to keep their private medical information confidential).

83. Under principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and members of the Class. Defendant has

failed to keep Plaintiff's and Class members' private medical information confidential and to implement industry standard data management and security measures to secure patients' private medical information, and under such circumstances, Defendant's retention of the benefit without payment would be unjust.

84. Accordingly, Mercy has received money from Plaintiff and the Class through the unlawful practices alleged herein, which in equity and good conscience should be returned.

COUNT III
Breach of Confidence
(On behalf of Plaintiff and the Ohio Subclass)

85. Plaintiff incorporates by reference the foregoing allegations as if fully set forth herein.

86. Plaintiff and members of the Ohio Subclass are residents of the State of Ohio.

87. In leaving its WebStation systems vulnerable, Defendant has made unauthorized and unprivileged disclosure to a third party of nonpublic medical information that a physician or hospital has learned within a physician-patient relationship.

88. Plaintiff's and Ohio Subclass members' private medical information that is accessible through Defendant's WebStation system is nonpublic medical information. Defendant learned of that information through a physician-patient relationship.

89. Plaintiff and members of the Ohio Subclass did not and have not provided consent to Defendant to disclose their nonpublic medical information to any third party in the way described herein.

90. Defendant's WebStation system has the JBoss Vulnerability, which was publicly disclosed in 2013. Since the JBoss Vulnerability has been publicly disclosed, Defendant has not updated or patched its systems to protect against it. As such, Defendant has acted intentionally by

failing to mitigate the JBoss Vulnerability and by exposing Plaintiff's and Ohio Subclass members' nonpublic medical information.

91. Plaintiff, on his own behalf and on behalf of the Ohio Subclass, seeks restitution, damages resulting from Defendant's breach of confidence, and to recover the costs of suit, including reasonable attorneys' fees.

COUNT IV
Violations of the Ohio Consumer Sales Protection Act
Ohio Rev. Code § 1345.09(D)
(On behalf of Plaintiff and the Ohio Subclass)

92. Plaintiff incorporates by reference the foregoing allegations as if fully set forth herein.

93. The Ohio Consumer Sales Protection Act (the "Ohio CSPA") prohibits suppliers from using "unfair or deceptive act or practice in connection with a consumer transaction" that occur "before, during, or after the transaction."

94. Defendant, Plaintiff, and each member of the Class is a "Person" as defined by Ohio Rev. Code § 1345.01(B) because they are each an individual or a corporation, government, governmental subdivision or agency, business trust, estate, trust, partnership, association, cooperative, or other legal entity.

95. Defendant is a "Supplier" as defined by Ohio Rev. Code §1345.01(C) because it is a seller or other person engaged in the business of effecting or soliciting consumer transactions, whether or not the person deals directly with the consumer.

96. Plaintiff and each member of the Class entered in to a "Consumer Transaction" as defined by Ohio Rev. Code §1345.01(A) because they purchased goods and services from Defendant for primarily personal, family, or household use. The Consumer Transactions do not include transactions between Plaintiff and members of the Class and any physicians because

Defendant is not a physician.

97. Plaintiff and each member of the Ohio Subclass is a consumer as defined by Ohio Rev. Code § 1345.01(D) because they are each a person who engaged in a consumer transaction with Defendant, a supplier.

98. Defendant continuously violates the CSPA because it has failed to implement basic security protocols thereby leaving Plaintiff's and the Ohio Subclass's private medical information at risk of further unauthorized disclosure. Defendant's actions are unfair because Mercy makes representations to consumers that it will keep their private medical information secure, Mercy receives payments (by and through Plaintiff and the Ohio Subclass paying their medical bills) to keep that information secure, and Mercy is obligated under federal law to employ safeguards to secure the private medical information.

99. Specifically, Defendant's actions violated the Ohio CSPA in at least the following respects:

- a. Violating 1345.02(B)(1) by representing that its medical services have sponsorship, approval, performance characteristics, accessories, uses, or benefits that they does not have; and
- b. Violating 1345.02(B)(2) by representing that its medical services are of a particular standard, quality, grade, style, prescription, or model, even when they are not.

100. In the course of its consumer transactions, Defendant has exposed the private medical records of tens of thousands of Ohio residents. Moreover, Mercy continuously maintains and ventures to obtain additional private medical information from the public in the State of Ohio, yet fails to adequately protect the public's private medical information, putting tens of

thousands of Ohio residents at risk of having their information disclosed without authorization. Without an injunction, thousands of consumers will be adversely affected by Defendant's conduct.

101. Plaintiff and members of the Class paid Mercy medical fees for medical treatment, and Mercy received and has knowledge of that payment. The medical fees that Plaintiff and the Class (directly or indirectly) paid to Mercy are (or should have been) used by Mercy, in part, to pay for the administrative costs of data management and security. However, Plaintiff and the Class did not receive the full benefit of the transaction and Mercy unfairly profits by not providing the paid-for services.

102. As a direct and proximate result of Defendant's unfair and/or deceptive conduct and its continuing unfair and/or deceptive conduct, Plaintiff and members of the Ohio Subclass have suffered injury because Mercy exposed their private medical information on its websites; they have suffered a diminished value of the Mercy services they received; and they are threatened with irreparable loss of the integrity of their private medical information and further injury and damages from the theft of that information.

103. Defendant's actions will continue unless enjoined by this Court. Plaintiff and members of the Ohio Subclass are likely to succeed on the merits, are without adequate remedies at law, are threatened with irreparable loss, injury, and damages unless the Court grants the equitable relief requested, and the equitable relief requested is also in the public interest.

104. Plaintiff and members of the Ohio Subclass will suffer substantially more from the denial of an order enjoining Defendant from further unfair or deceptive conduct than the Defendant would suffer from its issuance.

105. Plaintiff, on his own behalf and on behalf of the Ohio Subclass, seeks to enjoin

further violations by preventing Defendant from operating its network connected patient medical information portals (e.g., WebStation) until it implements industry standard security protocols to protect Plaintiff and Ohio Subclass's private medical information and recover the costs of suit, including reasonable attorneys' fees.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Lindsey Williams-Diggins, on behalf of himself and members of the Class, prays for the following relief:

- a. A preliminary injunction:
 - i. requiring Defendant to disconnect its servers from external networks (e.g., the internet) until it can implement industry standard procedures to make Plaintiff's and the Class's private medical information confidential;
 - ii. requiring Defendant to inform patients who have their private medical information accessible on Defendant's websites that they face a threat of further unauthorized disclosure due to Mercy's substandard security measures; and
 - iii. compelling Defendant to allow an independent third-party firm to conduct a security audit of its systems to ensure the integrity of patients' private medical information and determine the extent of any data breach that may have already occurred.

b. An order certifying this case as a class action on behalf of the Class defined above, appointing Lindsey Williams-Diggins as representative of the Class, and appointing his counsel as class counsel; and,

- c. An order:

- i. Declaring that Defendant's conduct, as set out above, constitutes a breach of contract, unjust enrichment, breach of confidence, and a violation of the Ohio CSPA and making the preliminary injunction permanent;
- ii. Awarding reasonable attorney's fees and expenses;
- iii. Awarding pre- and post-judgment interest, to the extent allowable; and,
- iv. Award such other and further relief as equity and justice may require.

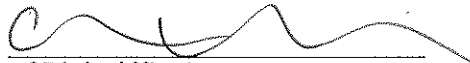
JURY DEMAND

Plaintiff requests trial by jury of all claims that can be so tried.

Respectfully Submitted,

LINDSEY WILLIAMS-DIGGINS, individually
and on behalf of all others similarly situated,

Dated: August 2, 2016

By: 
One of Plaintiff's Attorneys

Cathleen M. Bolek (0059884)
Bolek Besser Glesius, LLC
Monarch Centre, Suite 302
5885 Landerbrook Drive
Cleveland, Ohio 44124
Tel: 216.464.3004
Fax: 866.542.0743
cbolek@bolekbesser.com

Rafey S. Balabanian*
rbalabanian@edelson.com
Eve-Lynn J. Rapp*
erapp@edelson.com
EDELSON PC
123 Townsend Street
San Francisco, California 94107
Tel: 415.212.9300
Fax: 415.373.9435

Benjamin S. Thomassen*
bthomassen@edelson.com
EDELSON PC
350 North LaSalle Street, 13th Floor
Chicago, Illinois 60654
Tel: 312.589.6370
Fax: 312.589.6378
*Pro hac vice admission to be sought